SECS 1025

LABO Balayage/scanning

noté sur 19 points – 10% de la note finale

À rendre pour lundi 14 octobre 2024

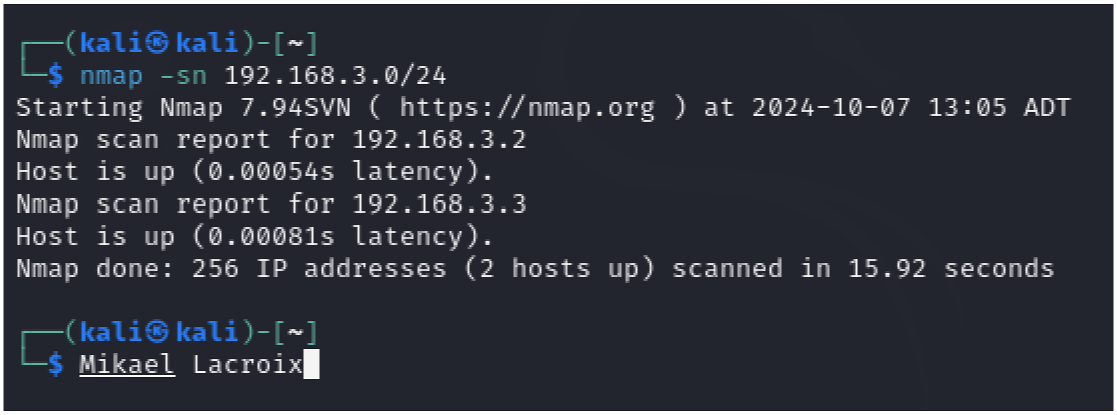
Rédigé par : Mikael Lacroix
Type de cours : SECS1025
Enseignant :
Pascal Perenon
Établissement : Collège Communautaire du Nouveau-Brunswick (CCNB)

Objectif du laboratoire : tester les techniques de balayage/scanning et d'énumérations.

Pour ce laboratoire vous avez besoin d'une VM kali et d'une VM Metasploitable2 sous un **réseau interne fermé** de VirtualBox. Les VM ne doivent pas pourvoir communiquer avec Internet ou la machine hôte (système qui exécute VirtualBox).

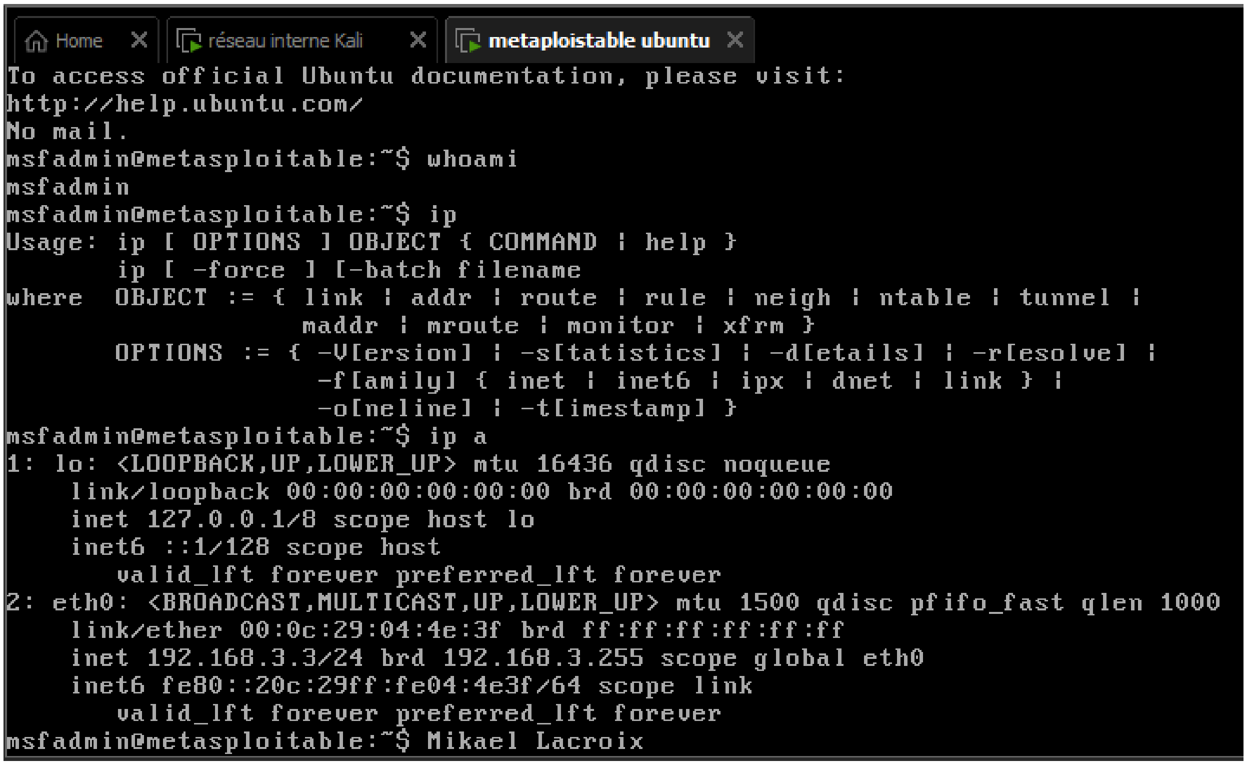
Exercice 1: Metasploitable2

1. Quelle est la commande Nmap pour découvrir les hôtes accessibles sur le réseau interne (192.168.2.0/24) ? Capture écran du résultat : 2 hosts



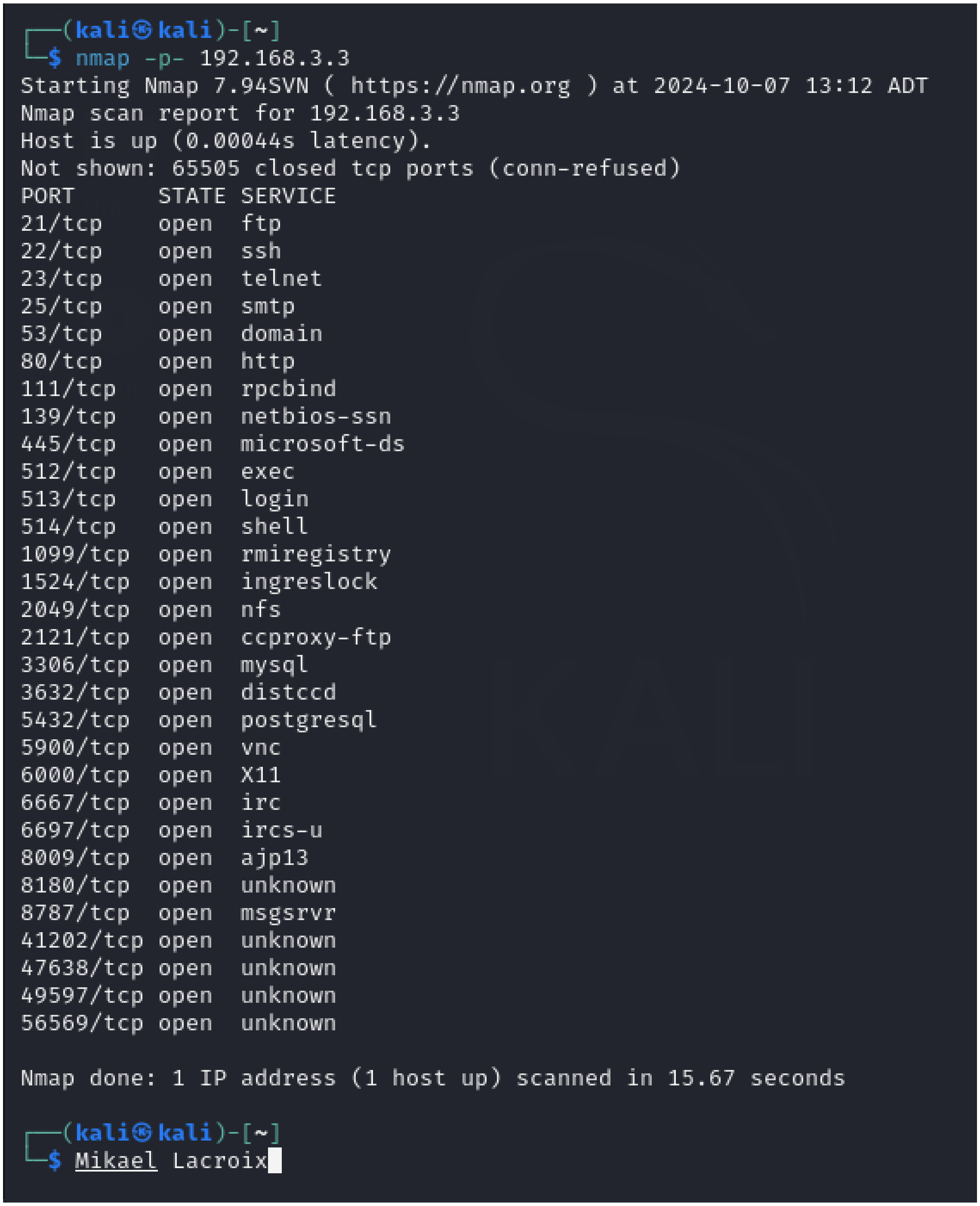
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.3.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:05 ADT
Nmap scan report for 192.168.3.2
Host is up (0.00054s latency).
Nmap scan report for 192.168.3.3
Host is up (0.00081s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 15.92 seconds

┌──(kali㉿kali)-[~]
└─$ Mikael Lacroix
```

2. Quelle est l'adresse IP de la VM metasploitable2 (sur le réseau interne) ? Capture écran du résultat. 192.168.3.3



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] [-batch filename
where  OBJECT := { link | addr | route | rule | neigh | ntable | tunnel |
                   maddr | mroute | monitor | xfrm }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -f[amily] { inet | inet6 | ipx | dnet | link } |
                    -o[neline] | -t[imestamp] }
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:04:4e:3f brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.3/24 brd 192.168.3.255 scope global eth0
    inet6 fe80::20c:29ff:fe04:4e3f/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ Mikael Lacroix
```

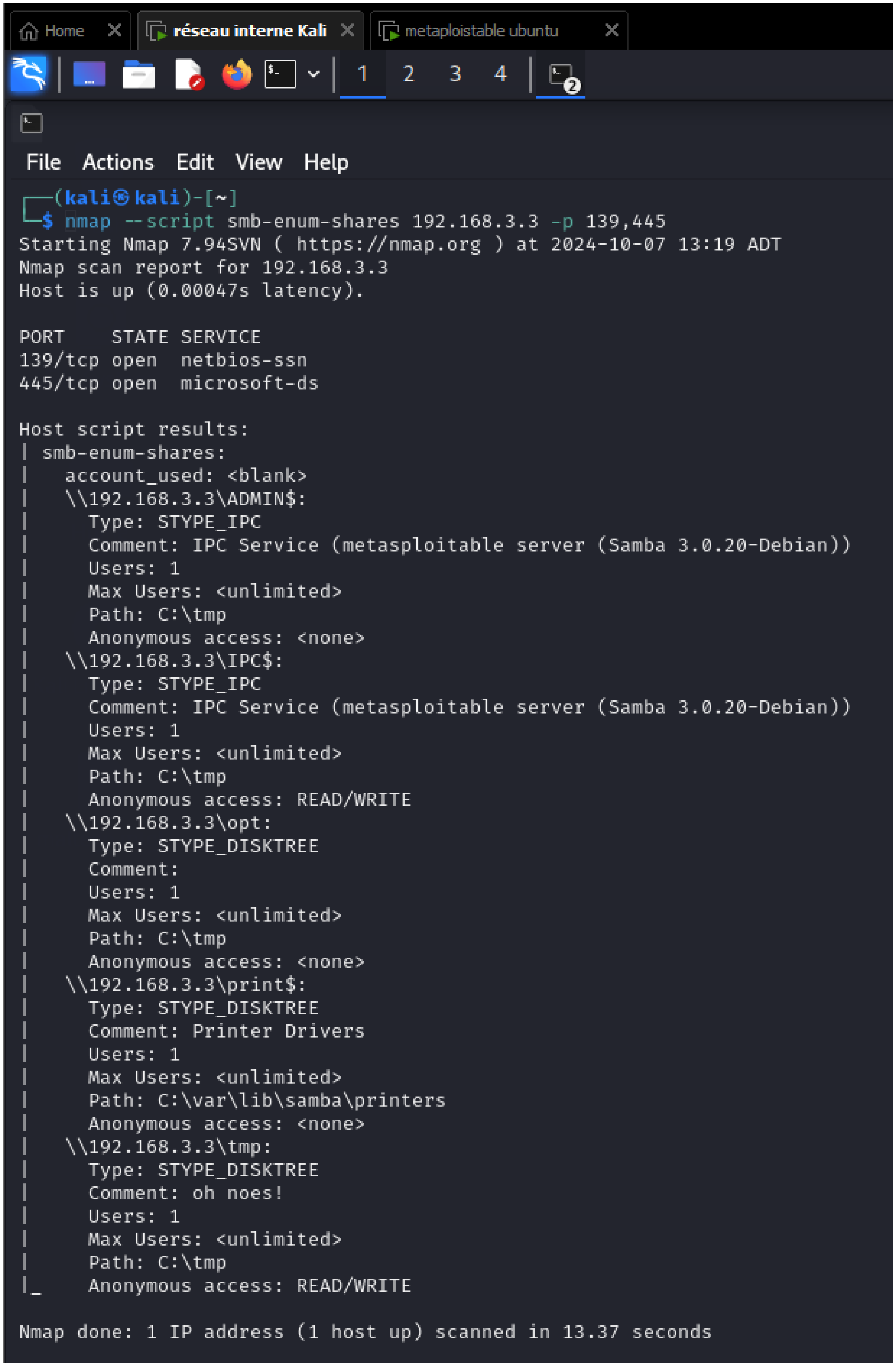
3. Quelle est la commande Nmap pour rechercher les ports ouverts sur la cible Metasploitable2 ? Capture écran du résultat : nmap -p- 192.168.3.3



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.3.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:12 ADT
Nmap scan report for 192.168.3.3
Host is up (0.00044s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
41202/tcp open  unknown
47638/tcp open  unknown
49597/tcp open  unknown
56569/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.67 seconds

┌──(kali㉿kali)-[~]
└─$ Mikael Lacroix
```

4. Combien de ports sont-ils ouverts ?
   30 Ports

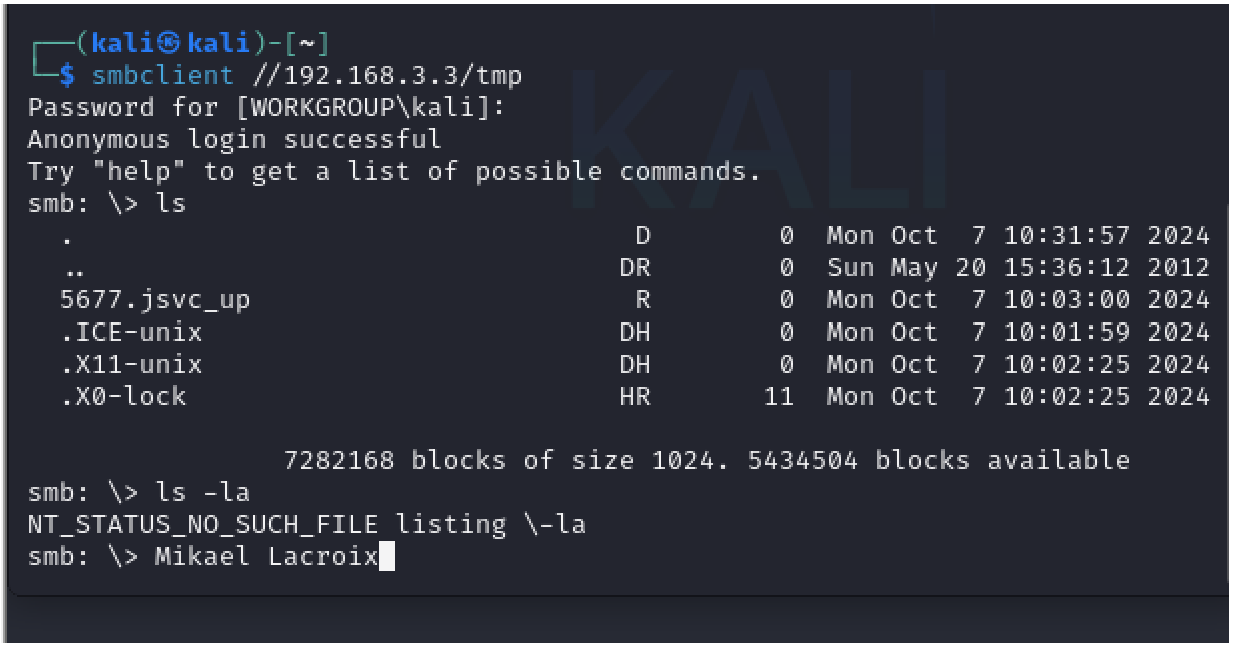
5. Quelle est la commande Nmap pour faire l’énumération des ressources partagées (shares) du service SMB ?
   nmap –script smb-enum-shares 192.168.3.3 -p 139,445



```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-enum-shares 192.168.3.3 -p 139,445
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:19 ADT
Nmap scan report for 192.168.3.3
Host is up (0.00047s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\192.168.3.3\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.3.3\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\192.168.3.3\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.3.3\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|   \\192.168.3.3\tmp:
|     Type: STYPE_DISKTREE
|     Comment: oh noes!
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|_    Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

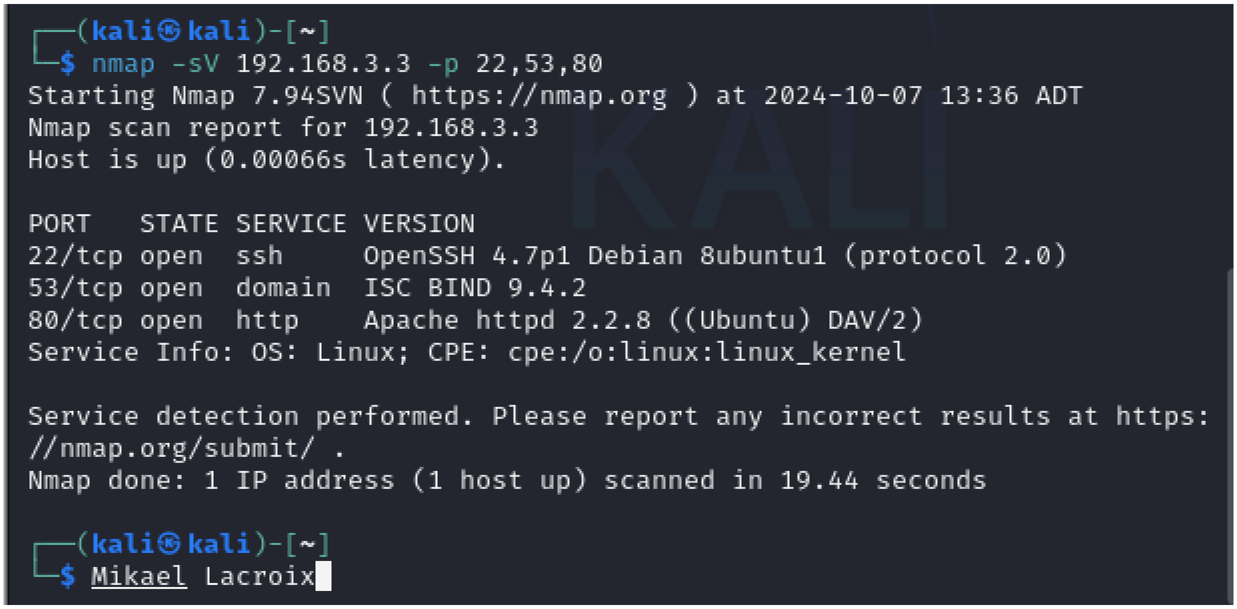
6. Parmi ces ressources partagées, laquelle attire votre attention (voir comment) ?
   192.168.3.3\tmp:

7. Quel utilitaire sous Kali permet de se connecter sur un partage SMB ? Connectez-vous sur le partage de la question précédente. Faites une capture écran :



```
┌──(kali㉿kali)-[~]
└─$ smbclient //192.168.3.3/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                       D        0  Mon Oct  7 10:31:57 2024
  ..                                     DR        0  Sun May 20 15:36:12 2012
  5677.jsvc_up                            R        0  Mon Oct  7 10:03:00 2024
  .ICE-unix                              DH        0  Mon Oct  7 10:01:59 2024
  .X11-unix                              DH        0  Mon Oct  7 10:02:25 2024
  .X0-lock                               HR       11  Mon Oct  7 10:02:25 2024

                7282168 blocks of size 1024. 5434504 blocks available
smb: \> ls -la
NT_STATUS_NO_SUCH_FILE listing \-la
smb: \> Mikael Lacroix
```

8. Quelle est la version des services sur les ports 22, 53, 80 ?
   Port 22: OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
   Port 53: ISC BIND 9.4.2
   Port 80: Apache httod 2.2.8 ((ubuntu) DAV/2)



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.3.3 -p 22,53,80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:36 ADT
Nmap scan report for 192.168.3.3
Host is up (0.00066s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
53/tcp open  domain  ISC BIND 9.4.2
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.44 seconds

┌──(kali㉿kali)-[~]
└─$ Mikael Lacroix
```

9. Quelle commande Nmap permet d'avoir des informations sur le service port 21 ?

   Nmap –script discovery 192.168.3.3 -p 21

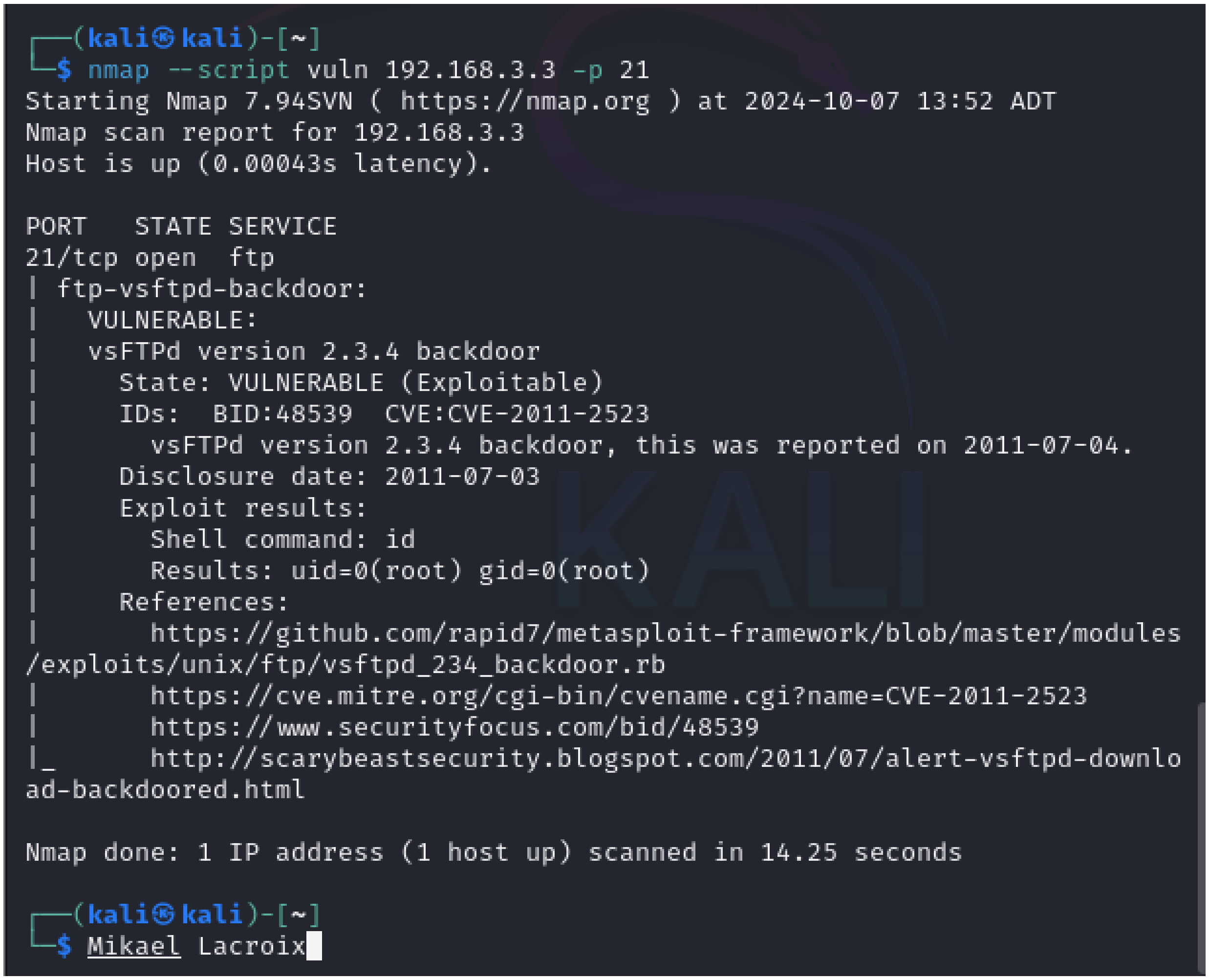
10. Quel script Nmap permet de tester si le service FTP est exploitable en mode anonyme ? Capture écran du résultat sur le port 21 :

    Nmap –script ftp-anon 192.168.3.3 -p 21

11. Quelle commande Nmap permet de détecter une vulnérabilité dans le service du port 21? Nmap –script vuln 192.168.3.3 -p 21

12. Quelle est l'identité CVE ID de la vulnérabilité de ce port ? Capture écran :

    CVE-2011-2523

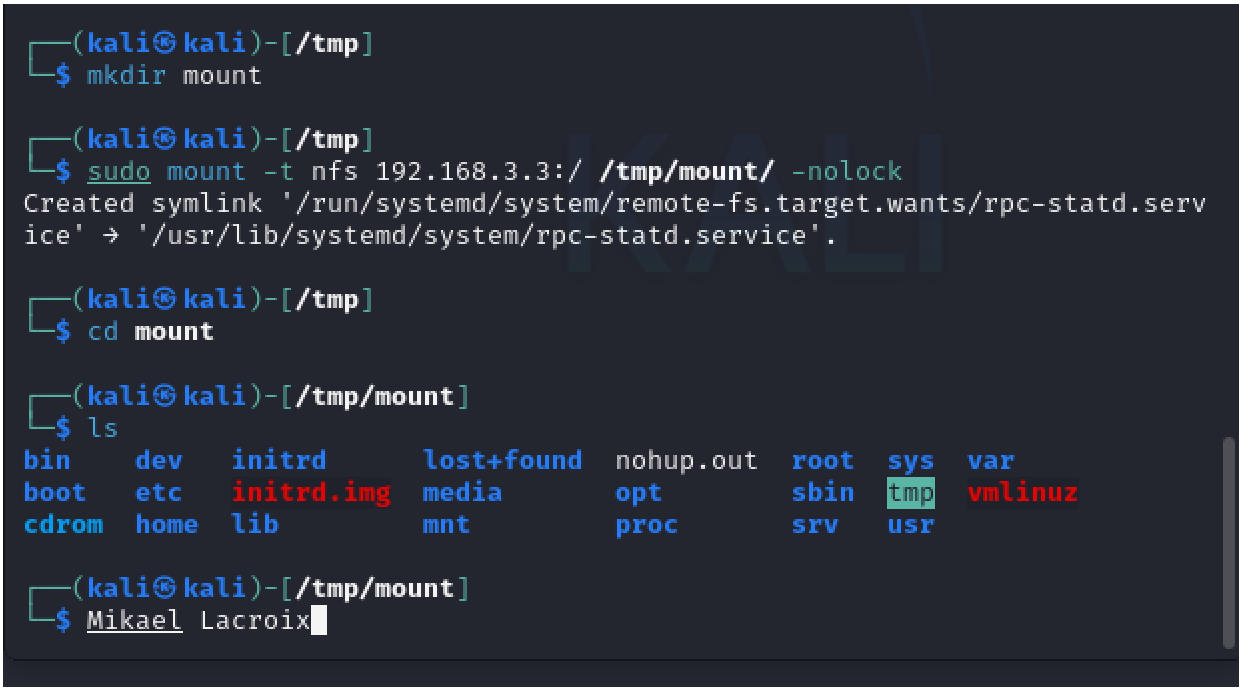


```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.3.3 -p 21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 13:52 ADT
Nmap scan report for 192.168.3.3
Host is up (0.00043s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules
/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-downlo
ad-backdoored.html

Nmap done: 1 IP address (1 host up) scanned in 14.25 seconds

┌──(kali㉿kali)-[~]
└─$ Mikael Lacroix
```

13. Quelle application Kali permet de lister les partages du service NFS ?

Nmap –script nfs-showmount 192.168.3.3 et showmount -e 192.168.3.3

14. Quelle commande kali permet de monter un partage NFS un dossier sur KALI ? Capture écran :



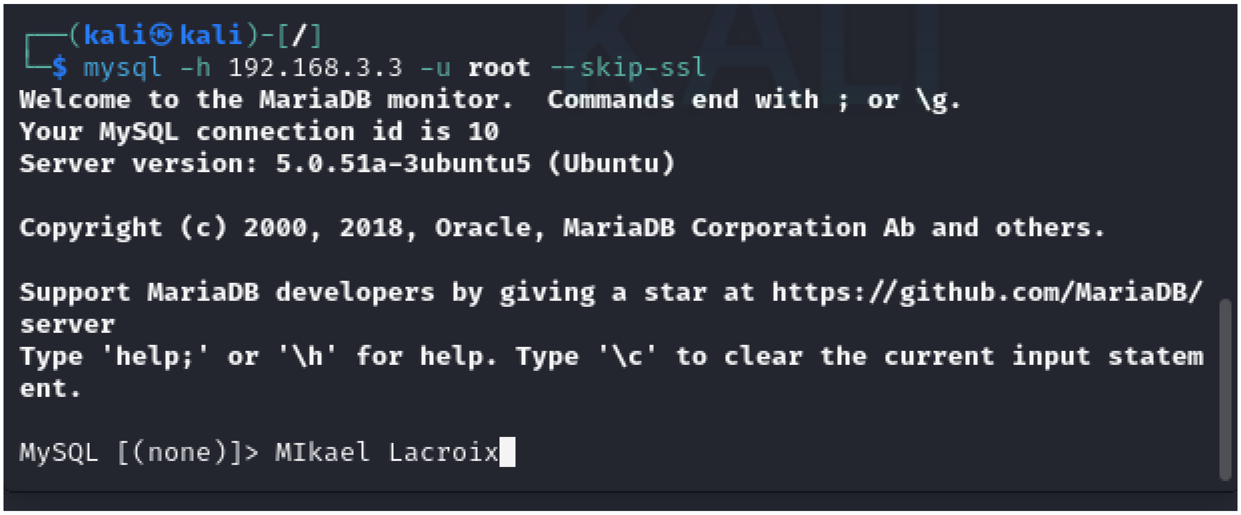
```
┌──(kali㉿kali)-[/tmp]
└─$ mkdir mount

┌──(kali㉿kali)-[/tmp]
└─$ sudo mount -t nfs 192.168.3.3:/ /tmp/mount/ -nolock
Created symlink '/run/systemd/system/remote-fs.target.wants/rpc-statd.serv
ice' → '/usr/lib/systemd/system/rpc-statd.service'.

┌──(kali㉿kali)-[/tmp]
└─$ cd mount

┌──(kali㉿kali)-[/tmp/mount]
└─$ ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr

┌──(kali㉿kali)-[/tmp/mount]
└─$ Mikael Lacroix
```

15. Quelle application Kali permet de trouver les logins/mot de passes en ligne ?
hydra

16. En utilisant cette application, créez la commande qui permet de trouver le mot de passe pour l’utilisateur root du service mysql sur metasploitable2
Hydra -t 4 -l root -P /usr/share/wordlists/rockyou.txt.gz -vV 192.168.3.3 mysql

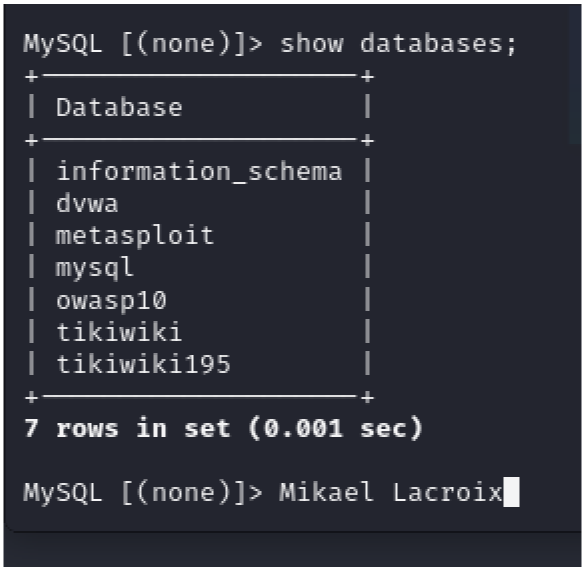
17. Avec le login root et le mot de passe que vous avez trouvé, comment pouvez-vous vous connecter sur le serveur mysql de la cible ?

Aucun mot de passe



```
┌──(kali㉿kali)-[/]
└─$ mysql -h 192.168.3.3 -u root --skip-ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/
server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statem
ent.

MySQL [(none)]> MIkael Lacroix
```

18. Lorsque vous êtes connectés au service mysql, affichez la liste des bases de données (capture écran) :



```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.001 sec)

MySQL [(none)]> Mikael Lacroix
```

19. Utilisez l'application Nikto pour détecter une vulnérabilité du serveur sur le port 80. Quelle est la commande utilisée ? Quelle est la vulnérabilité découverte du serveur web ? Capture écran :

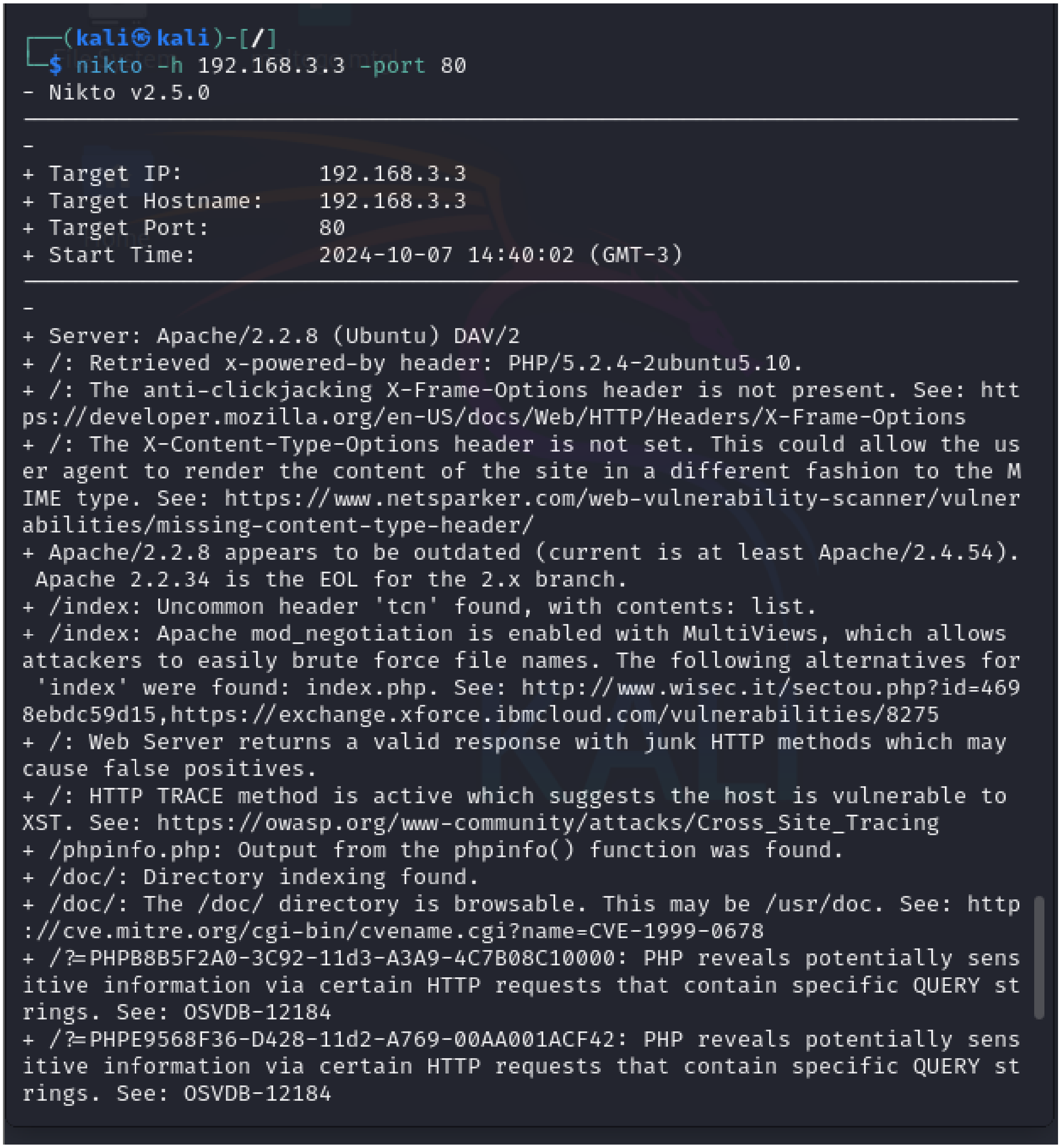
Commande : nikto -h 192.168.3.3 -port 80

-Apache outdated

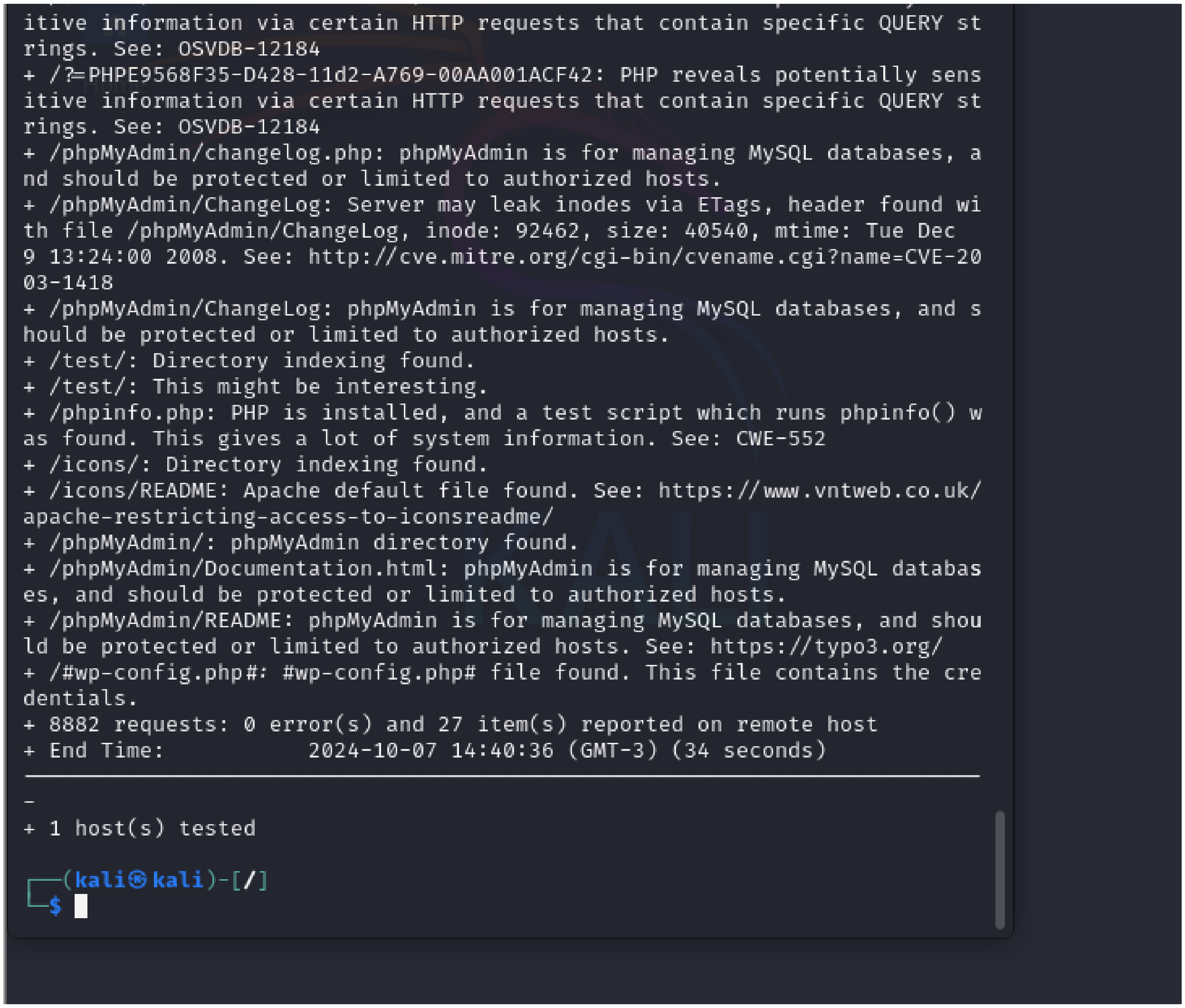
-http trace method is active wich suggests the host is vulnerable to xst

-Apache mod-negociation is enabled with multiviews, wich allows attackers to easily brute force file names.

-php admin config file found



```
┌──(kali㉿kali)-[/]
└─$ nikto -h 192.168.3.3 -port 80
- Nikto v2.5.0
---------------------------------------------------------------------------
-
+ Target IP:          192.168.3.3
+ Target Hostname:    192.168.3.3
+ Target Port:        80
+ Start Time:         2024-10-07 14:40:02 (GMT-3)
---------------------------------------------------------------------------
-
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: htt
ps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the us
er agent to render the content of the site in a different fashion to the M
IME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulner
abilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54).
 Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows
attackers to easily brute force file names. The following alternatives for
 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=469
8ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may
cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to
XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http
://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sens
itive information via certain HTTP requests that contain specific QUERY st
rings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sens
itive information via certain HTTP requests that contain specific QUERY st
rings. See: OSVDB-12184
```



```
itive information via certain HTTP requests that contain specific QUERY st
rings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sens
itive information via certain HTTP requests that contain specific QUERY st
rings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, a
nd should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found wi
th file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec
9 13:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-20
03-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and s
hould be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() w
as found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/
apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databas
es, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and shou
ld be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the cre
dentials.
+ 8882 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2024-10-07 14:40:36 (GMT-3) (34 seconds)
---------------------------------------------------------------------------
-
+ 1 host(s) tested

┌──(kali㉿kali)-[/]
└─$ 
```